UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/658,149	09/09/2003	Michael Darweesh	MSFT-2569/305143.1	5682

41505 7590 03/17/2008

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
PALIWAL, YOGESH	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
03/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/658,149	DARWEESH ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on 12/19/2008 has been entered. Applicant has amended claims 5 and 25. Currently claims 1-30 are pending in this application. Any well known art statements made in the prior office action not argued by applicant is taken as admittance of prior art as per MPEP 2144.03.
- Examiner acknowledges clarification of claim language of claims 5 and 25 for minor informalities. As a result, all claim objections previously presented are withdrawn.

Response to Arguments

1. Applicant's arguments filed on 12/19/2007 have been fully considered but they are not persuasive for following reasons:

- Regarding Claim 1, applicant argues that, "For example attention is drawn to that portion of the Office action which alleges that Auerbach's "Column 6, lines 15-27, "terms and conditions" and also a list of keys for all encrypted parts as disclosed at Column 6, lines 1-5)" anticipates a portion of Applicants' claim 1 that pertains to a manifest "comprising one or more rules governing what may be loaded into an address space of the software object." However, Applicants respectfully submit that the cited portions of Auerbach make no mention of addresses, let alone an "address space" as pertinent to Applicants' claim 1."

➢ In response, examiner would like to point out that examiner has pointed out at column 6, lines 15-27, for the limitation that recites "manifest comprising one or more rule governing what may be loaded into an address space of the software object". The cited part recites "Include terms and conditions such as fingerprinting and watermarking instructions 205 and pricing matrix 206. Encrypt any parts or sub-parts if necessary (and include their encrypted PEKs). As before

associate encrypted parts with their encrypted PEKs.". The terms and conditions defines if any part is encrypted or not encrypted and also provide correspond PRKs for the encrypted part, therefore terms and conditions in other words govern what part of the cryptographic envelope the end user is allowed access. Applicant is further emphasizing on the fact that Auerbach makes no mention of addresses, let along and "address space". In reply, examiner would like to point out that when end user loads any content of this cryptographic envelope, it is inherent that it is loaded into the address space of the software object [movie player for example] which is operating on the cryptographic envelope. Specification also provides the definition of address space as being "a region of memory that is available for use by software while software is executing" (see paragraph 0029). *In other words it is not possible for the end user to see the preview file without first loading it into the address space of the movie player in his/her computer*. Terms and conditions defines what parts are encrypted and what parts are not encrypted and since the encrypted parts are encrypted, it is interpreted as a rule governing what may be loaded into an address space because without PEKs, part that are encrypted cannot be loaded into the address space because of the mere fact that they are encrypted.

- Applicant further argues that, "In contrast, the cited portions of Auerbach describe certain elements (fingerprinting and watermarking instructions 205, pricing matrix 206, list 209 etc.) that are contained inside Auerbach's cryptographic envelope. Consequently, Applicants respectfully assert that Auerbach's disclosure shows what are contained inside an envelope but not **where** these contents are to be loaded in terms of an address space, or in other words, what can be loaded into an envelope but not what can be loaded into a **specific** address space. At least for the reasons described above, Applicants respectfully submit that the rejection fails to satisfy the

requirements necessary for a proper rejection under 35 U.S.C. 102(b) and hereby request withdrawal of the rejection followed by allowance of claim 1."

- In response, examiner would like to point out the alleged claimed limitation of "manifest comprising one or more rule governing **what** may be loaded into an address space of the software object". From the claim language it is clear the manifest govern **what** may be loaded into an address space of the software object and does not govern **where** [within any specific address space] it should be loaded within an address space of the software object as argued by applicant. The arguments about cryptographic content not being loaded into the address space is not found persuasive, because content have to first be loaded into a address space of the software for execution of the contents and even tough Auerbach does not explicitly discloses that contents are loaded into the address space of the software, examiner assert that this is inherent since content such as preview clip cannot be viewed by the end user without the contents of the preview clip be first loaded onto the address space of the movie player software.

- Regarding Claim 3, applicant argues that "In rejecting Applicants' claim 3, the Office action asserts that Applicants' "...one or more modules may be loaded into the address space of the software object" is disclosed in Auerbach's "Column 6, lines 12-14, "Include in the cryptographic envelope clear text parts such as "teasers ", abstract, and a table of content 201." Applicants respectfully traverse this assertion. In Auerbach's col. 6, lines 30-48, certain details pertaining to distribution and use of his cryptographic envelope are disclosed. Specifically, it is disclosed that the cryptographic envelope is distributed to a user who can browse the plain text "teaser" 201 portion of the envelope and then decide if he/she wishes to purchase a part encryption key (PEK). Applicants respectfully submit that Auerbach's clear text teaser (located inside his

envelope) which is directed to encouraging the purchase of a PEK (for accessing encrypted material inside his envelope) bears no relevance to Applicants' claim 3 incorporating "a specification" for generating a manifest that is then used for identifying a particular "acceptable" module that may be loaded into a particular address space.

- Auerbach at Column 6, lines 12-14 clearly discloses that some content of the cryptographic envelope are not encrypted so that they can be used as “teasers”. During the envelope creation it is implied that some information needs to be delivered to the envelope creator to identify the teaser part and that would result in not encrypting that part. The mere fact of teaser not being encrypted is sufficient to understand that teaser can be played by the end user and as explained above, the teaser much first be loaded into the address space before user can actually see it on his screen. Therefore, examiner is equating the clear text "teaser" of Auerbach to the first one of said one or more module that may be loaded into the address space of the software object.

- Regarding Claim 4, applicant argues that, “In rejecting Applicants' claim 4, the Office action asserts that "it is implied that this information (as disclosed in Auerbach Column 5, lines 63-67) needs to be delivered to the envelope creator and can be interpreted as a specification identifying one or more modules may not be loaded into the address space of the software object [encrypted parts]." Applicants respectfully traverse such a conclusion especially in connection with a rejection under 35 U.S.C. 102(b) where no question of obviousness must be present. A further impropriety in the Office action assertion lies in the fact that assuming arguendo that Auerbach does indeed incorporate providing information pertaining to one particular module amongst several modules (claim 4 cites "one of said one or more modules") it is improper to presume that

this information pertains to a module that that may not be loaded and more specifically not loaded into a particular address space."

- Examiner is not trying to suggest that this rejection is obviousness type rejection; the wording used by the examiner is misinterpreted by the applicant. Examiner is simply saying that the limitation is implicitly disclosed by the Auerbach reference. MPEP (chapter 2105) defines that "Disclosure may be express, implicit, or inherent", therefore in this case examiner is just mapping a limitation which is implicitly disclosed by Auerbach reference. Further, examiner would like to point out that the limitation "one of said one or more modules" that may not be loaded is clearly taught by Auerbach at Fig. 3, "Encrypted Doc Part1"). As explained by Auerbach these parts are encrypted therefore in other word these parts cannot be viewed by the end user without first decrypting them with PEKs stored in terms and conditions field of the cryptographic envelope. Therefore, Encrypted Doc Part1 as depicted in Fig. 3 cannot be loaded into the end user's computer by default, and this reads onto the claimed limitation of module that may not be loaded. Furthermore, as explained above the limitation of module being loaded into the address space is inherent for the reasons provided above.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12,13, 14, 15, 16, 17, 18, 19, 20, 21, 23, 24, 25, 26, 27, 29, 30 are rejected under 35 U.S.C. 102(b) as being anticipated by Auerbach et al. (US 5,673,316), hereinafter Auerbach.

Regarding **Claim 1**, Auerbach discloses a method of generating a manifest that governs the execution of a software object **(Column 1, lines 39-41, "This invention describes a method for the creation, distribution, and sale of digital information using the methods and techniques of secure cryptographic envelopes")**, the method comprising:

receiving a specification indicative of requirements for the execution of the software object, the specification referring to one or more components **(Column 5, lines 55-62, "Assemble information parts to be included in the cryptographic envelope", also at Column 4, lines 9-18, since the envelope contains both encrypted and unencrypted parts, during cryptographic envelope creation, system must know which part needs to be encrypted, as a result it is implied that this information needs to be delivered to the envelope creator and can be interpreted as a specification indicative of requirements for the execution of the software object, also the part keys included in envelope can be interpreted as specification indicative of requirements for the execution of the software object)**;

Note: Auerbach discloses that contents of the envelope are not restricted to movies of music and discloses at Column 4, lines 4-8 that "[D]document parts are the "contents". Some examples of

document parts are abstracts, table of contents, figures, tables, and texts, They Could also be portions of an **executable program, a library of sub-routines, software modules, or object components**".

generating a manifest based on said specification, including accessing said one or more components **(Column 6, lines 15-27, "Create a list 209 of information parts, listing all the parts assembled and computing a secure hash of each of the parts listed")**, said manifest comprising one or more rules governing what may be loaded into an address space of the software object **(Column 6, lines 15-27, "terms and conditions" and also a list of keys for all encrypted parts as disclosed at Column 6, lines 1-5, Note: "terms and conditions" govern what components of the envelope are encrypted or not encrypted. End user can load unencrypted contents for preview; Auerbach does not explicitly disclose that contents are first loaded into the address space of the software object. However, it is inherent that contents are loaded into the address space of the software object [movie player for example] which is operating on the cryptographic envelope. Specification also provides the definition of address space as being "a region of memory that is available for use by software while software is executing" (see paragraph 0029). In other words it is not possible for the end user to see the preview file without first loading it into the address space of the movie player in his/her computer. For detailed explanation please refer to the "Response to arguments")**.

Regarding **Claim 2**, the rejection of claim 1 is incorporated and Auerbach further discloses wherein said specification identifies one or more modules **(As established above in the rejection of claim 1, since the envelope contains both encrypted and unencrypted parts, during cryptographic envelope creation, system must know which part needs to be encrypted, as a result it is implied that this information needs to be delivered to the envelope creator and is**

interpreted as a specification identifying one of more modules) , and wherein generating the manifest comprises including, in said manifest, the identities of the one or more modules identified in the specification **(Column 5, 19-26, "We apply a secure hash function, MessageDigest5 (MD5) (see. e.g., [1] for details), to each part included in a cryptographic envelope and create a list. Referring to Fig. 3, each entry in the list contains the part name or reference 302 and a secure hash 301 of the information part corresponding to the part name")**

Regarding **Claim 3**, the rejection of claim 2 is incorporated and Auerbach further discloses wherein said specification indicates that a first one of said one or more modules may be loaded into the address space of the software object **(Column 6, lines 12-14, "Include in the cryptographic envelope clear text parts such as "teasers", abstract, and a table of content 201." also at Fig. 3, Numerals 302 and 301, Abstract is listed under list of parts)** and wherein generating the manifest comprises including the identity of said first one of said one or more modules on list of acceptable modules **(Fig. 3, Numerals 302 and 301)**

Regarding **Claim 4**, the rejection of claim 2 is incorporated and Auerbach further discloses wherein said specification indicates that a first one of said one or more modules may not be loaded into the address space of the software object **(Column 5, lines 63-67, as established above in the rejection of claim 1, since the envelope contains both encrypted and unencrypted parts, during cryptographic envelope creation, system must know which part needs to be encrypted, as a result it is implied that this information needs to be delivered to the envelope creator and is interpreted as a specification identifying one of more modules may not be loaded into the**

address space of the software object [encrypted parts]), and wherein generating the manifest comprises including in the manifest a datum that identifies said first one of said one or more modules **(Fig. 3, "Encrypted Doc Part 1")**

Regarding **Claim 5**, the rejection of claim 4 is incorporated and Auerbach further discloses wherein said datum comprises a hash of said first one of said one or more modules **(Fig. 3, MD5 of "Encrypted doc part 1", which is 24FDEC234...")**

Regarding **Claim 6**, the rejection of claim 2 is incorporated and Auerbach further discloses wherein said specification indicates whether said manifest will contain hashes of said one or more modules **(Fig. 3, "MD5 of Part").**

Regarding **Claim 7**, the rejection of claim 1 is incorporated and Auerbach further discloses wherein said one or more components comprise a key **(Column 2, lines 20-22, "With this invention, each of the information parts is encrypted with a corresponding part encryption key to generate an encrypted information part" and at Column 2, lines 26-28, "The envelope, then, includes the encrypted information parts, the unencrypted information parts, the encrypted part encryption keys and list of parts")**,

wherein said specification indicates either that modules signed with said key may be loaded into said address space or that modules signed with said key may not be loaded into said address space **(Column 2, lines 28-36, "Finally, the list of parts is signed with a secret key to produce a**

signature, and this signature is also included in the envelope. The integrity of the list can be checked using a second public key associated with the secret key that was used to sign the list. The integrity of any one information part can be checked by computing a second hash on the part and comparing the second hash with the corresponding hash for the part in the list."), and

wherein generating said manifest comprises: retrieving said key from a file identified in said specification; and including said key in said manifest **(Column 2, lines 26-28, "The envelope, then, includes the encrypted information parts, the unencrypted information parts, the encrypted part encryption keys and the list of parts")**.

Regarding **Claim 8**, the rejection of claim 1 is incorporated and Auerbach further discloses wherein said one or more components comprise a module **(Column 4, lines 4-8, "Documents parts are abstracts, table of contents, figures, tables, and texts, They could also be portions of an executable program, a library of subroutines, software modules, or object components")**, wherein said specification indicates that said module may not be loaded into said address space **(Column 5, lines 63-67, as established above in the rejection of claim 1, since the envelope contains both encrypted and unencrypted parts, during cryptographic envelope creation, system must know which part needs to be encrypted, as a result it is implied that this information needs to be delivered to the envelope creator and can be interpreted as a specification identifying one of more modules may not be loaded into the address space of the software object [encrypted parts])**, and wherein generating said manifest comprises: computing a hash of said module **(Column 5, lines 19-21, "We apply a secure hash function, MessageDigest5 (MD5) (see, e.g., [1] for details), to each part included in a cryptographic envelope and create a list.")**; and including said hash in

said manifest **(Fig. 3, Numeral 209, "MD5 of Part" is included in the BOM section of cryptographic envelope)**.

Regarding **claim 9**, the rejection of claim 1 is incorporated and Auerbach further discloses wherein said generating act comprises: based on said specification, creating a data structure representative of said specification; and generating said manifest based on said data structure **(Fig. 3, "BOM", and at Column 5, lines 13-34)**

Regarding **Claim 10**, the rejection of claim 1 is incorporated and Auerbach further discloses wherein receiving a key associated with a vendor or distributor of said software object **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)")**;

signing said manifest with said to produce a digital signature **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)");** and

including said digital signature in said manifest **(Fig. 2, Numeral 208, "Signature on list of parts") and at Column 2, lines 28-30, "Finally, the list of parts is signed with a secret key to produce a signature, and this signature is also included in the envelope.").**

Regarding **Claim 12**, Auerbach discloses computer implemented method of generating a manifest, the method comprising:

parsing a specification of requirements to be included in the manifest, the requirements defining a policy that governs what can be loaded into an address space of a software object associated with the manifest **(Column 5, lines 55-62, "Assemble information parts to be included in the cryptographic envelope", also at Column 4, lines 9-18, since the envelope contains both encrypted and unencrypted parts, during cryptographic envelope creation, system must know which part needs to be encrypted, as a result it is implied that this information needs to be delivered to the envelope creator and can be interpreted as a specification indicative of requirements for the execution of the software object, also the part keys included in envelope can be interpreted as specification indicative of requirements for the execution of the software object)**;

accessing one or more components that are identified by the specification and that are external to the specification **(Column 5, lines 63-67, "1-c – Generate random PEKs (part encryption keys) 202, one for each part to be encrypted. 1-d – Encrypt document parts with their respective PEKs to form the encrypted parts (203, 204, 205), which are included in the cryptographic envelope")**; and

generating a manifest based on at least one of the accessed objects **(Column 6, lines 15-27, "terms and conditions" and also a list of keys for all encrypted parts as disclosed at Column 6, lines 1-5)**.

Regarding **Claim 13**, the rejection of claim 12 is incorporated and Auerbach further discloses wherein said one or more components comprise an executable module **(Column 4, lines 4-8, "Documents parts are abstracts, table of contents, figures, tables, and texts, They could also be**

portions of an executable program, a library of subroutines, software modules, or object components"), and

wherein generating said manifest comprises:

including in said manifest an identification of said executable module and an indication that either: said executable module may be loaded into said address space; or said executable module may not be loaded into said address space **(Fig. 3, "list of parts" that list abstract which can be loaded into address space because it is not encrypted and Encrypted Doc Part 1 which cannot be loaded into address space because it is encrypted)**.

Regarding **Claim 14**, the rejection of claim 14 is incorporated and Auerbach further discloses wherein said identification of said executable module comprises a hash of said executable module **(Fig. 3, Numeral 209, "MD5 of part")**

Regarding **Claim 15**, the rejection of claim 13 is incorporated and Auerbach further discloses wherein said one or more components comprise a key **(Column 2, lines 20-22, "With this invention, each of the information parts is encrypted with a corresponding part encryption key to generate an encrypted information part" and at Column 2, lines 26-28, "The envelope, then, includes the encrypted information parts, the unencrypted information parts, the encrypted part encryption keys and list of parts")**, wherein said specification indicates either that modules signed with said key may be loaded into said address space or that modules signed with said key may not be loaded into said address space **(Column 2, lines 28-36, "Finally, the list of parts is signed with a secret key to**

produce a signature, and this signature is also included in the envelope. The integrity of the list can be checked using a second public key associated with the secret key that was used to sign the list. The integrity of any one information part can be checked by computing a second hash on the part and comparing the second hash with the corresponding hash for the part in the list."), and wherein generating said manifest comprises:

retrieving said key from a file identified in said specification **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)")**; and

including said key in said manifest **(Column 6, lines 15-27, "terms and conditions" and also a list of keys for all encrypted parts as disclosed at Column 6, lines 1-5)**.

Regarding **Claim 16**, the rejection of claim 12 is incorporated and Auerbach further discloses receiving a key associated with a vendor or distributor of said software object **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)")**; signing said manifest with said to produce a digital signature **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)")**; and including said digital signature in said manifest **(Fig. 2, Numeral 208, "Signature on list of parts") and at Column 2, lines 28-30, "Finally, the list of parts is signed with a secret key to produce a signature, and this signature is also included in the envelope.").**

Regarding **Claim 17**, Auerbach discloses a method of specifying constraints on the use of software **(Column 1, lines 39-41, "This invention describes a method for the creation, distribution,**

and sale of digital information using the methods and techniques of secure cryptographic envelopes") comprising:

creating a specification concerning what may be loaded into an address space of the software, the specification referring to one or more components that are external to the software and external to the specification **(Column 5, lines 55-62, "Assemble information parts to be included in the cryptographic envelope", also at Column 4, lines 9-18, since the envelope contains both encrypted and unencrypted parts, during cryptographic envelope creation, system must know which part needs to be encrypted, as a result it is implied that this information needs to be delivered to the envelope creator and can be interpreted as a specification indicative of requirements for the execution of the software object, also the part keys included in envelope can be interpreted as specification indicative of requirements for the execution of the software object);**

using a manifest generation tool to generate a manifest based on the specification **(Column 6, lines 15-27, "terms and conditions" and also a list of keys for all encrypted parts as disclosed at Column 6, lines 1-5)**, wherein the manifest generation tool does at least one of:

including, in said manifest, data from one of said one or more components **(Fig. 2, Numerals 201, 203, 204)**; or

computing a value based on one of said one or more components and including the computed value in said manifest **(Fig. 3, Numeral 209, "MD5 of part")**; and

distributing the generated manifest with the software **(Fig. 2, Numeral 206, "terms and Conditions" and Numeral 207, "BOM")**, wherein the manifest comprises rules describing what may be

loaded into the address space of the software **(Column 6, lines 15-27, "terms and conditions" and also a list of keys for all encrypted parts as disclosed at Column 6, lines 1-5)**.

Regarding **Claim 18**, the rejection of claim 17 is incorporated and Auerbach further discloses wherein said one or more components comprises a module, wherein said specification indicates either that said module may be loaded into said address space or that said module may not be loaded into said address space **(Column 5, lines 63-67, as established above in the rejection of claim 1, since the envelope contains both encrypted and unencrypted parts, during cryptographic envelope creation, system must know which part needs to be encrypted, as a result it is implied that this information needs to be delivered to the envelope creator and can be interpreted as a specification identifying one of more modules may or may not be loaded into the address space of the software object, based on whether the part is encrypted or not])**, and wherein said manifest generation tool does at least one of: including an identifier of said module in said manifest; or computing a hash of said module and including the hash in said manifest **(Column 5, 19-26, "We apply a secure hash function, MessageDigest5 (MD5) (see. e.g., [1] for details), to each part included in a cryptographic envelope and create a list. Referring to Fig. 3, each entry in the list contains the part name or reference 302 and a secure hash 301 of the information part corresponding to the part name")**.

Regarding **Claim 19**, the rejection of claim 17 is incorporated and Auerbach further discloses wherein said one or more components comprise a key **(Column 2, lines 20-22, "With this invention,**

each of the information parts is encrypted with a corresponding part encryption key to generate an encrypted information part" and at Column 2, lines 26-28, "The envelope, then, includes the encrypted information parts, the unencrypted information parts, the encrypted part encryption keys and list of parts"), wherein said specification indicates either that modules signed with said key may be loaded into said address space or that modules signed with said key may not be loaded into said address space **(Column 2, lines 28-36, "Finally, the list of parts is signed with a secret key to produce a signature, and this signature is also included in the envelope. The integrity of the list can be checked using a second public key associated with the secret key that was used to sign the list. The integrity of any one information part can be checked by computing a second hash on the part and comparing the second hash with the corresponding hash for the part in the list.")**, and wherein said manifest generation tool retrieves said key from a file identified in said specification, and includes a certificate for said key in said manifest **(Column 2, lines 26-28, "The envelope, then, includes the encrypted information parts, the unencrypted information parts, the encrypted part encryption keys and the list of parts")**.

Regarding **Claim 20**, the rejection of claim 17 is incorporated and Auerbach further discloses said manifest generation tool creates an intermediate data structure representative of said specification, and generates said manifest based on said intermediate data structure **(Fig. 3, "BOM", and at Column 5, lines 13-34)**.

Regarding **Claim 21,** the rejection of claim 17 is incorporated and Auerbach further discloses receiving a key associated with a vendor or distributor of said software object **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)")**;

signing said manifest with said to produce a digital signature **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)");** and

including said digital signature in said manifest **(Fig. 2, Numeral 208, "Signature on list of parts") and at Column 2, lines 28-30, "Finally, the list of parts is signed with a secret key to produce a signature, and this signature is also included in the envelope.").**

Regarding **Claim 23**, Auerbach discloses a system for generating a manifest (Fig. 1) comprising:

a first parser that receives a manifest specification indicative of requirements for a manifest, the first parser generating a representation of said requirements, said requirements relating to what may be loaded into an address space of a software object, said specification referring to one or more components external to said software and external to said specification **(Column 5, lines 55-62, "Assemble information parts to be included in the cryptographic envelope", also at Column 4, lines 9-18, since the envelope contains both encrypted and unencrypted parts, during cryptographic envelope creation, system must know which part needs to be encrypted, as a result it is implied that this information needs to be delivered to the envelope creator and can be interpreted as a specification indicative of requirements for the execution of the software object, also the part keys included in envelope can be interpreted as specification indicative of requirements for the execution of the software object)**;

a first manifest generator that generates a manifest based on said representation and includes in said manifest information contained in, or computed based on, said one or more components **(Column 6, lines 15-27, "terms and conditions" and also a list of keys for all encrypted parts as disclosed at Column 6, lines 1-5).**

Regarding **Claim 24**, the rejection of claim 23 is incorporated and Auerbach further discloses said one or more components comprise a module **(Column 4, lines 4-8, "Documents parts are abstracts, table of contents, figures, tables, and texts, They could also be portions of an executable program, a library of subroutines, software modules, or object components")**, and wherein said first manifest generator generates said manifest by including, in said manifest, a datum that identifies said module **(Fig. 3, "list of parts" that list abstract which can be loaded into address space because it is not encrypted and Encrypted Doc Part 1 which cannot be loaded into address space because it is encrypted).**

Regarding **Claim 25**, the rejection of claim 24 is incorporated and Auerbach further discloses wherein said datum comprises a hash of said module **(Fig. 3, Numeral 209, "MD5 of Part")**

Regarding **Claim 26**, the rejection of claim 23 is incorporated and Auerbach further discloses wherein said one or more components comprise a key **(Column 2, lines 20-22, "With this invention, each of the information parts is encrypted with a corresponding part encryption key to generate an encrypted information part" and at Column 2, lines 26-28, "The envelope, then, includes the**

encrypted information parts, the unencrypted information parts, the encrypted part encryption keys and list of parts"), wherein said specification indicates either that modules signed with said key may be loaded into said address space or that modules signed with said key may not be loaded into said address space **(Column 2, lines 28-36, "Finally, the list of parts is signed with a secret key to produce a signature, and this signature is also included in the envelope. The integrity of the list can be checked using a second public key associated with the secret key that was used to sign the list. The integrity of any one information part can be checked by computing a second hash on the part and comparing the second hash with the corresponding hash for the part in the list.")**, and wherein generating said manifest comprises:

retrieving said key from a file identified in said specification **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)")**; and

including said key in said manifest **(Column 6, lines 15-27, "terms and conditions" and also a list of keys for all encrypted parts as disclosed at Column 6, lines 1-5)**.

Regarding **Claim 27**, the rejection of claim 23 is incorporated and Auerbach further discloses receiving a key associated with a vendor or distributor of said software object **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)")**; signing said manifest with said to produce a digital signature **(Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)")**; and including said digital signature in said manifest **(Fig. 2, Numeral 208, "Signature on list of parts") and at Column 2,**

lines 28-30, "Finally, the list of parts is signed with a secret key to produce a signature, and this signature is also included in the envelope.").

Regarding **Claim 29**, the rejection of claim 23 is incorporated and Auerbach further discloses a second parser that receives a manifest specification indicative of requirements for a manifest **(Column 9, lines 14-47, "Step 4: Buy Server Response")**, the second parser generating a representation of said requirements in the same format as said first parser **(Column 10, lines 9-34, "BSR")**, wherein said first parser parses specifications in a first format and second parser parses specifications in a second format different from said first format **(Column 10, lines 27-31)**, and wherein first manifest generator generates said manifest based on a representation produced either by said first parser or said second parser **(Column 10, lines 32-34, "Include transformed terms and conditions and other restrictions on the use of the documents in BSR 605. 4-h – Send BSR to user")**.

Regarding **Claim 30**, the rejection of claim 23 is incorporated and Auerbach further discloses a second manifest generator that generates a manifest based on said representation, wherein said first manifest generator generates a manifest in a first format and second manifest generator generates a manifest in a second format different from said first format **(Column 3, lines 45-53, "The creation event is usually done off-line by the content provider because of anticipated needs for a collection of digital documents to be super distributed. Alternatively, it could be triggered by a user request. In this case the cryptographic envelope would be created specifically for the user,**

and the cryptographic envelope may contain certain information specific to the user or the request").

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 11, 22 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Auerbach in view of Watanabe et al. (US 2002/0108041 A1), hereinafter Watanabe.

Regarding **Claims 11, 22 and 28**, the rejections of claims 1, 17 and 27 are incorporated and Auerbach discloses signing a manifest using the private key of the vendor or distributor (Column 5, lines 27-28, "The list is then digitally signed with a secret key known only to the DS (Document Server)"). Auerbach does not explicitly discloses using hardware security module to sign manifest, said hardware security module being adapted to apply a key associated with a vendor or distributor of said software object without revealing said key outside said hardware security module.

However, Watanabe, in the same field of endeavor of cryptography, discloses signing digital document with private key of the signing party without revealing private key outside hardware security module **(Paragraph 0195, One of the approaches to solve the problems of security assurance and enhanced computing speed is the use of a hardware security module (HSM) in holding the signature keys (or private keys) and executing signature processing.")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to use in he system of Auerbach, during a creation of cryptographic envelopes, use a hardware security module, as taught by Watanabe to provider highly temper resistant and security for the private key of the vendor **(Watanabe, Paragraph 0195)**

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yogesh Paliwal/
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135